

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-016384

(43)Date of publication of application : 19.01.1996

(51)Int.Cl.

G06F 9/06
G06F 12/14

(21)Application number : 06-152053

(71)Applicant : MATSUSHITA ELECTRIC IND CO
LTD

(22)Date of filing : 04.07.1994

(72)Inventor : MIYAJI MITSUKO
OMORI MOTOJI
MATSUZAKI NATSUME

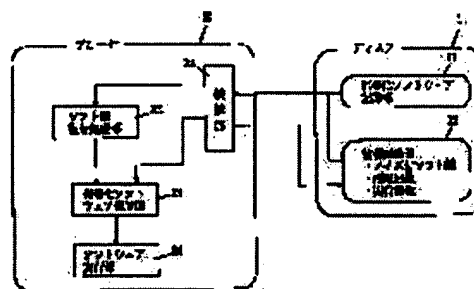
(54) CONTROLLING SYSTEM FOR EXECUTION OF SOFTWARE

(57)Abstract:

PURPOSE: To provide the software execution control system with which the execution of a software by an executing equipment can be limited according to previously decided execution conditions such as the available frequency.

CONSTITUTION: A disk 1 is connected to a connecting part 21 of a player 2. The connecting part 21 reads the limited number of times and the number of times of execution for software keys with noise recorded in an information recording part 12. At such a time, '1' is added to the number of times of execution. The read software key with noise is decoded by a software key decode processing part 22 while using the similarly read limited number of times and the number of times of execution.

At such a time, only when the number of times of execution is less than the limited number of times, the software key decode processing part 22 normally decodes the software key with noise. On the other hand, a ciphered software recorded in a ciphered software recording part 11 is read out and deciphered by a ciphered software deciphering part 23 while using the software key decoded in advance. The deciphered software is executed by a software executing part 24.



THIS PAGE BLANK (USPTO)

LEGAL STATUS

[Date of request for examination] 15.11.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3399638

[Date of registration] 21.02.2003

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-16384

(43) 公開日 平成 8 年 (1996) 1 月 19 日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 9/06	5 5 0 L	7230-5B		
	A	7230-5B		
12/14	3 2 0 F			

審査請求 未請求 請求項の数 9 O L (全 10 頁)

(21) 出願番号 特願平6-152053

(22) 出願日 平成 6 年 (1994) 7 月 4 日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 宮地 充子

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 大森 基司

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 松崎 なつめ

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

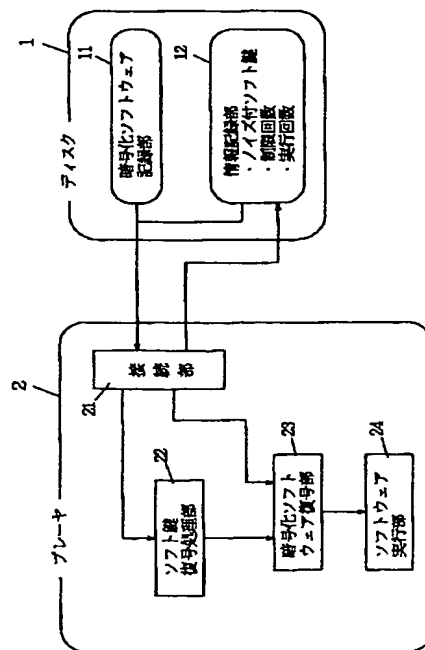
(74) 代理人 弁理士 小笠原 史朗

(54) 【発明の名称】 ソフトウェア実行制御システム

(57) 【要約】

【目的】 予め定めた使用回数等の実行条件に従って、実行器でのソフトウェアの実行を制限し得るソフトウェア実行制御システムを提供することである。

【構成】 ディスク 1 は、プレーヤ 2 の接続部 21 に接続される。接続部 21 は、情報記録部 12 に記録されているノイズ付きソフト鍵と制限回数と実行回数とを読み込む。このとき、実行回数は 1 つ増やされる。読み込まれたノイズ付きソフト鍵は、同じく読み込まれた制限回数と実行回数を用いて、ソフト鍵復号処理部 22 で復号される。このとき、ソフト鍵復号処理部 22 は、実行回数が制限回数以下の場合にのみ、ノイズ付きソフト鍵を正常に復号する。また、暗号化ソフトウェア記録部 11 に記録されている暗号化ソフトウェアを読み出し、先に復号化されたソフト鍵を用いて、暗号化ソフトウェア復号部 23 で復号する。復号されたソフトウェアは、ソフトウェア実行部 24 で実行される。



1

【特許請求の範囲】

【請求項 1】 記録媒体に格納されたソフトウェアを実行器で実行する際に、当該ソフトウェアの実行回数を制限するシステムであって、前記記録媒体には、少なくとも、暗号化されたソフトウェアと、暗号化されたソフト鍵と、予め定められた制限回数と、今までに前記ソフトウェアを実行した回数である実行回数とが格納されており、前記記録媒体から前記暗号化されたソフトウェアと、前記暗号化されたソフト鍵と、前記制限回数と、前記実行回数とを読み出す読み出し手段と、前記読み出し手段によって読み出された前記暗号化されたソフト鍵を、前記制限回数および前記実行回数をを用いて復号化するソフト鍵復号処理手段と、前記読み出し手段によって読み出された前記暗号化されたソフトウェアを、前記ソフト鍵復号処理手段によって復号化されたソフト鍵を用いて復号化する暗号化ソフトウェア復号手段と、前記暗号化ソフトウェア復号手段によって復号化されたソフトウェアを実行するソフトウェア実行手段と、前記読み出し手段による読み出し動作に関連して、前記記録媒体における前記実行回数を更新する実行回数更新手段とを備え、前記ソフト鍵復号処理手段は、前記実行回数が前記制限回数以下の場合にのみ、前記暗号化されたソフト鍵を正常に復号することを特徴とする、ソフトウェア実行制御システム。

【請求項 2】 前記読み出し手段と、前記ソフト鍵復号処理手段と、前記暗号化ソフトウェア復号手段と、前記ソフトウェア実行手段と、前記実行回数更新手段とは、前記実行器内に設けられている、請求項 1 に記載のソフトウェア実行制御システム。

【請求項 3】 前記ソフト鍵復号処理手段は、前記記録媒体を収納したカートリッジに関連して設けられ、前記読み出し手段と、前記暗号化ソフトウェア復号手段と、前記ソフトウェア実行手段と、前記実行回数更新手段とは、前記実行器内に設けられている、請求項 1 に記載のソフトウェア実行制御システム。

【請求項 4】 記録媒体に格納されたソフトウェアを実行器で実行する際に、当該ソフトウェアの実行回数を制限するシステムであって、前記記録媒体には、少なくとも、暗号化されたソフトウェアと、暗号化されたソフト鍵と、残りの実行可能回数を示す残高回数とが格納されており、前記記録媒体から前記暗号化されたソフトウェアと、前記暗号化されたソフト鍵と、前記残高回数とを読み出す読み出し手段と、前記読み出し手段によって読み出された前記暗号化されたソフト鍵を、前記残高回数をを用いて復号化するソフト鍵復号処理手段と、

2

前記読み出し手段によって読み出された前記暗号化されたソフトウェアを、前記ソフト鍵復号処理手段によって復号化されたソフト鍵を用いて復号化する暗号化ソフトウェア復号手段と、

前記暗号化ソフトウェア復号手段によって復号化されたソフトウェアを実行するソフトウェア実行手段と、前記読み出し手段による読み出し動作に関連して、前記記録媒体における前記残高回数を更新する残高回数更新手段とを備え、

10 前記ソフト鍵復号処理手段は、前記残高回数が 1 以上の場合にのみ、前記暗号化されたソフト鍵を正常に復号することを特徴とする、ソフトウェア実行制御システム。

【請求項 5】 記録媒体に格納されたソフトウェアを実行器で実行する際に、当該ソフトウェアの実行回数を制限するシステムであって、

前記記録媒体には、少なくとも、暗号化されたソフトウェアと、ソフト鍵と、予め定められた制限回数と、今までに前記ソフトウェアを実行した回数である実行回数とが格納されており、

20 前記記録媒体から前記暗号化されたソフトウェアと、前記ソフト鍵と、前記制限回数と、前記実行回数とを読み出す読み出し手段と、

前記読み出し手段によって読み出された前記ソフト鍵を入力し、前記実行回数が前記制限回数以下の場合は当該ソフト鍵をそのまま出力し、前記実行回数が前記制限回数を越える場合は当該ソフト鍵に所定のノイズを付加して出力するフィルタ手段と、

前記読み出し手段によって読み出された前記暗号化されたソフトウェアを、前記フィルタ手段から出力されるソフト鍵を用いて復号化する暗号化ソフトウェア復号手段と、

前記暗号化ソフトウェア復号手段によって復号化されたソフトウェアを実行するソフトウェア実行手段と、前記読み出し手段による読み出し動作に関連して、前記記録媒体における前記実行回数を更新する実行回数更新手段とを備える、ソフトウェア実行制御システム。

【請求項 6】 記録媒体に格納されたソフトウェアを実行器で実行する際に、当該ソフトウェアの実行回数を制限するシステムであって、

40 前記記録媒体には、少なくとも、暗号化されたソフトウェアと、ソフト鍵と、残りの実行可能回数を示す残高回数とが格納されており、

前記記録媒体から前記暗号化されたソフトウェアと、前記ソフト鍵と、前記残高回数とを読み出す読み出し手段と、

前記読み出し手段によって読み出された前記ソフト鍵を入力し、前記残高回数が 1 以上の場合は当該ソフト鍵をそのまま出力し、前記残高回数が 0 以下の場合は当該ソフト鍵に所定のノイズを付加して出力するフィルタ手段と、

50

3

前記読み出し手段によって読み出された前記暗号化されたソフトウェアを、前記フィルタ手段から出力されるソフト鍵を用いて復号化する暗号化ソフトウェア復号手段と、

前記暗号化ソフトウェア復号手段によって復号化されたソフトウェアを実行するソフトウェア実行手段と、

前記読み出し手段による読み出し動作に関連して、前記記録媒体における前記残高回数を更新する残高回数更新手段とを備える、ソフトウェア実行制御システム。

【請求項 7】 記録媒体に格納されたソフトウェアを実行器で実行する際に、当該ソフトウェアの実行日時を制限するシステムであって、

前記記録媒体には、少なくとも、暗号化されたソフトウェアと、暗号化されたソフト鍵と、予め定められた実行停止日時とが格納されており、

現在の日時を計時するタイマ手段と、

前記記録媒体から前記暗号化されたソフトウェアと、前記暗号化されたソフト鍵と、前記実行停止日時とを読み出す読み出し手段と、

前記読み出し手段によって読み出された前記暗号化されたソフト鍵を、前記タイマ手段により計時された現在の日時および前記実行停止日時を用いて復号化するソフト鍵復号処理手段と、

前記読み出し手段によって読み出された前記暗号化されたソフトウェアを、前記ソフト鍵復号処理手段によって復号化されたソフト鍵を用いて復号化する暗号化ソフトウェア復号手段と、

前記暗号化ソフトウェア復号手段によって復号化されたソフトウェアを実行するソフトウェア実行手段とを備え、

前記ソフト鍵復号処理手段は、前記現在の日時が前記実行停止日時よりも時間的に前の場合にのみ、前記暗号化されたソフト鍵を正常に復号することを特徴とする、ソフトウェア実行制御システム。

【請求項 8】 記録媒体に格納されたソフトウェアを実行器で実行する際に、当該ソフトウェアの実行日時を制限するシステムであって、

前記記録媒体には、少なくとも、暗号化されたソフトウェアと、ソフト鍵と、予め定められた実行停止日時とが格納されており、

現在の日時を計時するタイマ手段と、

前記記録媒体から前記暗号化されたソフトウェアと、前記ソフト鍵と、前記実行停止日時とを読み出す読み出し手段と、

前記読み出し手段によって読み出された前記ソフト鍵を入力し、前記タイマ手段により計時された現在の日時が前記実行停止日時よりも時間的に前の場合は当該ソフト鍵をそのまま出力し、現在の日時が前記実行停止日時よりも時間的に後の場合は当該ソフト鍵に所定のノイズを付加して出力するフィルタ手段と、

4

前記読み出し手段によって読み出された前記暗号化されたソフトウェアを、前記フィルタ手段から出力されるソフト鍵を用いて復号化する暗号化ソフトウェア復号手段と、

前記暗号化ソフトウェア復号手段によって復号化されたソフトウェアを実行するソフトウェア実行手段とを備える、ソフトウェア実行制御システム。

【請求項 9】 暗号化されたソフトウェアと、暗号化されたソフト鍵と、予め定められた制限回数と、今までに前記ソフトウェアを実行した回数である実行回数とが格納された記録媒体に対し、前記制限回数を追加更新するためのシステムであって、

前記ソフトウェアの追加したい実行回数を入力する入力手段と、

前記記録媒体に格納された前記制限回数と前記実行回数との大小関係を考慮しつつ、前記入力手段から入力された追加実行回数に基づいて、前記制限回数の更新回数を演算する更新回数演算手段と、

前記更新回数演算手段により演算された更新回数によって、前記記録媒体に格納された前記制限回数を書き換える制限回数書き換え手段とを備える、追加更新システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、ソフトウェア実行制御システムに関し、より特定的には、記録媒体に格納されたソフトウェアを実行器で実行する際に、当該ソフトウェアの実行回数を制限するシステムに関する。

【0002】

【従来の技術】近年、種々のマルチメディア機器が開発され、ゲームや教育用のソフトウェアを始めとする多くの有償マルチメディアソフトウェアが販売されている。ところで、従来のソフトウェアは、使用回数或使用日数に制限がないため、販売側としてはユーザが無制限にそのソフトウェアを使用するものと推定して、その分高めにソフトウェアの販売価格を設定していた。

【0003】

【発明が解決しようとする課題】しかしながら、ユーザは、購入したソフトウェアを何度も何度も繰り返し使用するとは限らず、途中でその使用をやめてしまう場合も考えられる。例えば、ゲーム用のソフトウェアの場合、何回か実行すると飽きてしまって、再び使用することがなくなるかもしれない。また、他のソフトウェアについても、購入後に実行したが、その機能や使い勝手が自分の希望とするものと異なる場合、途中で使用をやめてしまう場合もある。

【0004】上記のような実状を何ら考慮することなく、全てのソフトウェアを常に高価格で販売することは、ユーザに対して過度の価格負担を強いることになり、健全な商取引上好ましくない。

5

【0005】それゆえに、本発明の目的は、予め定めた使用回数等の実行条件に従って、実行器でのソフトウェアの実行を制限し得るソフトウェア実行制御システムを提供することである。

【0006】本発明の他の目的は、上記実行条件を途中で更新できるような追加更新システムを提供することである。

【0007】

【課題を解決するための手段】請求項1に係る発明は、記録媒体に格納されたソフトウェアを実行器で実行する際に、当該ソフトウェアの実行回数を制限するシステムであって、記録媒体には、少なくとも、暗号化されたソフトウェアと、暗号化されたソフト鍵と、予め定められた制限回数と、今までにソフトウェアを実行した回数である実行回数とが格納されており、記録媒体から暗号化されたソフトウェアと、暗号化されたソフト鍵と、制限回数と、実行回数とを読み出す読み出し手段と、読み出し手段によって読み出された暗号化されたソフト鍵を、制限回数および実行回数を用いて復号化するソフト鍵復号処理手段と、読み出し手段によって読み出された暗号化されたソフトウェアを、ソフト鍵復号処理手段によって復号化されたソフト鍵を用いて復号化する暗号化ソフトウェア復号手段と、暗号化ソフトウェア復号手段によって復号化されたソフトウェアを実行するソフトウェア実行手段と、読み出し手段による読み出し動作に関連して、記録媒体における実行回数を更新する実行回数更新手段とを備え、ソフト鍵復号処理手段は、実行回数が制限回数以下の場合にのみ、暗号化されたソフト鍵を正常に復号することを特徴とする。

【0008】請求項2に係る発明は、請求項1の発明において、読み出し手段と、ソフト鍵復号処理手段と、暗号化ソフトウェア復号手段と、ソフトウェア実行手段と、実行回数更新手段とは、実行器内に設けられていることを特徴とする。

【0009】請求項3に係る発明は、請求項1の発明において、ソフト鍵復号処理手段は、記録媒体を収納したカートリッジに関連して設けられ、読み出し手段と、暗号化ソフトウェア復号手段と、ソフトウェア実行手段と、実行回数更新手段とは、実行器内に設けられていることを特徴とする。

【0010】請求項4に係る発明は、記録媒体に格納されたソフトウェアを実行器で実行する際に、当該ソフトウェアの実行回数を制限するシステムであって、記録媒体には、少なくとも、暗号化されたソフトウェアと、暗号化されたソフト鍵と、残りの実行可能回数を示す残高回数とが格納されており、記録媒体から暗号化されたソフトウェアと、暗号化されたソフト鍵と、残高回数とを読み出す読み出し手段と、読み出し手段によって読み出された暗号化されたソフト鍵を、残高回数を用いて復号化するソフト鍵復号処理手段と、読み出し手段によって

6

読み出された暗号化されたソフトウェアを、ソフト鍵復号処理手段によって復号化されたソフト鍵を用いて復号化する暗号化ソフトウェア復号手段と、暗号化ソフトウェア復号手段によって復号化されたソフトウェアを実行するソフトウェア実行手段と、読み出し手段による読み出し動作に関連して、記録媒体における残高回数を更新する残高回数更新手段とを備え、ソフト鍵復号処理手段は、残高回数が1以上の場合にのみ、暗号化されたソフト鍵を正常に復号することを特徴とする。

【0011】請求項5に係る発明は、記録媒体に格納されたソフトウェアを実行器で実行する際に、当該ソフトウェアの実行回数を制限するシステムであって、記録媒体には、少なくとも、暗号化されたソフトウェアと、ソフト鍵と、予め定められた制限回数と、今までにソフトウェアを実行した回数である実行回数とが格納されており、記録媒体から暗号化されたソフトウェアと、ソフト鍵と、制限回数と、実行回数とを読み出す読み出し手段と、読み出し手段によって読み出されたソフト鍵を入力し、実行回数が制限回数以下の場合には当該ソフト鍵をそのまま出力し、実行回数が制限回数を越える場合は当該ソフト鍵に所定のノイズを付加して出力するフィルタ手段と、読み出し手段によって読み出された暗号化されたソフトウェアを、フィルタ手段から出力されるソフト鍵を用いて復号化する暗号化ソフトウェア復号手段と、暗号化ソフトウェア復号手段によって復号化されたソフトウェアを実行するソフトウェア実行手段と、読み出し手段による読み出し動作に関連して、記録媒体における実行回数を更新する実行回数更新手段とを備えている。

【0012】請求項6に係る発明は、記録媒体に格納されたソフトウェアを実行器で実行する際に、当該ソフトウェアの実行回数を制限するシステムであって、記録媒体には、少なくとも、暗号化されたソフトウェアと、ソフト鍵と、残りの実行可能回数を示す残高回数とが格納されており、記録媒体から暗号化されたソフトウェアと、ソフト鍵と、残高回数とを読み出す読み出し手段と、読み出し手段によって読み出されたソフト鍵を入力し、残高回数が1以上の場合は当該ソフト鍵をそのまま出力し、残高回数が0以下の場合には当該ソフト鍵に所定のノイズを付加して出力するフィルタ手段と、読み出し手段によって読み出された暗号化されたソフトウェアを、フィルタ手段から出力されるソフト鍵を用いて復号化する暗号化ソフトウェア復号手段と、暗号化ソフトウェア復号手段によって復号化されたソフトウェアを実行するソフトウェア実行手段と、読み出し手段による読み出し動作に関連して、記録媒体における残高回数を更新する残高回数更新手段とを備えている。

【0013】請求項7に係る発明は、記録媒体に格納されたソフトウェアを実行器で実行する際に、当該ソフトウェアの実行日時を制限するシステムであって、記録媒体には、少なくとも、暗号化されたソフトウェアと、暗

7

号化されたソフト鍵と、予め定められた実行停止日時とが格納されており、現在の日時を計時するタイマ手段と、記録媒体から暗号化されたソフトウェアと、暗号化されたソフト鍵と、実行停止日時とを読み出す読み出し手段と、読み出し手段によって読み出された暗号化されたソフト鍵を、タイマ手段により計時された現在の日時および実行停止日時を用いて復号化するソフト鍵復号処理手段と、読み出し手段によって読み出された暗号化されたソフトウェアを、ソフト鍵復号処理手段によって復号化されたソフト鍵を用いて復号化する暗号化ソフトウェア復号手段と、暗号化ソフトウェア復号手段によって復号化されたソフトウェアを実行するソフトウェア実行手段とを備え、ソフト鍵復号処理手段は、現在の日時が実行停止日時よりも時間的に前の場合にのみ、暗号化されたソフト鍵を正常に復号することを特徴とする。

【0014】請求項8に係る発明は、記録媒体に格納されたソフトウェアを実行器で実行する際に、当該ソフトウェアの実行日時を制限するシステムであって、記録媒体には、少なくとも、暗号化されたソフトウェアと、ソフト鍵と、予め定められた実行停止日時とが格納されており、現在の日時を計時するタイマ手段と、記録媒体から暗号化されたソフトウェアと、ソフト鍵と、実行停止日時とを読み出す読み出し手段と、読み出し手段によって読み出されたソフト鍵を入力し、タイマ手段により計時された現在の日時が実行停止日時よりも時間的に前の場合は当該ソフト鍵をそのまま出力し、現在の日時が実行停止日時よりも時間的に後の場合は当該ソフト鍵に所定のノイズを付加して出力するフィルタ手段と、読み出し手段によって読み出された暗号化されたソフトウェアを、フィルタ手段から出力されるソフト鍵を用いて復号化する暗号化ソフトウェア復号手段と、暗号化ソフトウェア復号手段によって復号化されたソフトウェアを実行するソフトウェア実行手段とを備えている。

【0015】請求項9に係る発明は、暗号化されたソフトウェアと、暗号化されたソフト鍵と、予め定められた制限回数と、今までにソフトウェアを実行した回数である実行回数とが格納された記録媒体に対し、制限回数を追加更新するためのシステムであって、ソフトウェアの追加したい実行回数を入力する入力手段と、記録媒体に格納された制限回数と実行回数との大小関係を考慮しつつ、入力手段から入力された追加実行回数に基づいて、制限回数の更新回数を演算する更新回数演算手段と、更新回数演算手段により演算された更新回数によって、記録媒体に格納された制限回数を書き換える制限回数書き換え手段とを備えている。

【0016】

【作用】請求項1に係る発明においては、記録媒体には、少なくとも、暗号化されたソフトウェアと、暗号化されたソフト鍵と、予め定められた制限回数と、今までにソフトウェアを実行した回数である実行回数とが格納

8

される。そして、記録媒体から、暗号化されたソフトウェアと、暗号化されたソフト鍵と、制限回数と、実行回数とを読み出し、この読み出された暗号化されたソフト鍵を、ソフト鍵復号処理手段で制限回数および実行回数を用いて復号化する。このとき、ソフト鍵復号処理手段は、実行回数が制限回数以下の場合にのみ、暗号化されたソフト鍵を正常に復号する。また、記録媒体から読み出された暗号化されたソフトウェアを、復号化されたソフト鍵を用いて復号化し、この復号化されたソフトウェアをソフトウェア実行手段で実行する。また、記録媒体からの各データの読み出し動作に関連して、記録媒体における実行回数を更新する。従って、ソフトウェアの実行回数は、予め定められた回数に制限され、当該回数以上の実行を行うことは不可能である。その結果、販売店としては、販売時に定めた回数に見合う安い価格でソフトウェアパッケージを販売することが可能となり、その分ユーザの価格負担を軽減できる。

【0017】請求項2に係る発明においては、読み出し手段と、ソフト鍵復号処理手段と、暗号化ソフトウェア復号手段と、ソフトウェア実行手段と、実行回数更新手段とを、実行器内に設けるようにしている。

【0018】請求項3に係る発明においては、ソフト鍵復号処理手段を記録媒体を収納したカートリッジに関連して設け、読み出し手段と、暗号化ソフトウェア復号手段と、ソフトウェア実行手段と、実行回数更新手段とを、実行器内に設けるようにしている。

【0019】請求項4に係る発明においては、記録媒体には、請求項1の制限回数および実行回数に代えて、残りの実行可能回数を示す残高回数が格納されている。そして、ソフト鍵復号処理手段は、記録媒体から読み出された暗号化されたソフト鍵を、残高回数を用いて復号化する。このとき、ソフト鍵復号処理手段は、残高回数が1以上の場合にのみ、暗号化されたソフト鍵を正常に復号する。また、残高更新手段は、記録媒体からのデータの読み出し動作に関連して、記録媒体における残高回数を更新する。

【0020】請求項5に係る発明においては、記録媒体には、請求項1の暗号化されたソフト鍵に代えて、暗号化されていないソフト鍵が格納されている。そして、フィルタ手段は、記録媒体から読み出されたソフト鍵を入力し、実行回数が制限回数以下の場合は当該ソフト鍵をそのまま出力し、実行回数が制限回数を越える場合は当該ソフト鍵に所定のノイズを付加して出力する。また、暗号化ソフトウェア復号手段は、記録媒体から読み出された暗号化されたソフトウェアを、フィルタ手段から出力されるソフト鍵を用いて復号化する。

【0021】請求項6に係る発明においては、記録媒体には、請求項1の制限回数および実行回数に代えて、残りの実行可能回数を示す残高回数が格納され、また、暗号化されたソフト鍵に代えて、暗号化されていないソフト

9

ト鍵が格納されている。そして、フィルタ手段は、記録媒体から読み出されたソフト鍵を入力し、残高回数が1以上の場合は当該ソフト鍵をそのまま出力し、残高回数が0以下の場合は当該ソフト鍵に所定のノイズを付加して出力する。また、ソフトウェア復号手段は、記録媒体から読み出された暗号化されたソフトウェアを、フィルタ手段から出力されるソフト鍵を用いて復号化する。また、残高回数更新手段は、記録媒体からの各データの読み出し動作に関連して、記録媒体における残高回数を更新する。

【0022】請求項7に係る発明においては、記録媒体には、少なくとも、暗号化されたソフトウェアと、暗号化されたソフト鍵と、予め定められた実行停止日時とが格納される。そして、記録媒体から、暗号化されたソフトウェアと、暗号化されたソフト鍵と、実行停止日時とを読み出し、この読み出された暗号化されたソフト鍵を、タイマ手段により計時された現在の日時および実行停止日時を用いて復号化する。このとき、ソフト鍵復号処理手段は、現在の日時が実行停止日時よりも時間的に前の場合にのみ、暗号化されたソフト鍵を正常に復号する。また、記録媒体から読み出された暗号化されたソフトウェアを、復号化されたソフト鍵を用いて復号化し、この復号化されたソフトウェアをソフトウェア実行手段で実行する。従って、ソフトウェアの実行期間を予め定められた日数に制限することができ、当該日数以上の実行を行うことは不可能である。その結果、販売店としては、販売時に定めた日数に見合う安い価格でソフトウェアパッケージを販売することが可能となり、その分ユーザの価格負担を軽減できる。

【0023】請求項8に係る発明においては、記録媒体には、請求項7の暗号化されたソフトウェアに代えて、暗号化されていないソフトウェアが格納されている。そして、フィルタ手段は、記録媒体から読み出されたソフト鍵を入力し、タイマ手段により計時された現在の日時が実行停止日時よりも時間的に前の場合は当該ソフト鍵をそのまま出力し、現在の日時が実行停止日時よりも時間的に後の場合は当該ソフト鍵に所定のノイズを付加して出力する。また、ソフトウェア復号手段は、記録媒体から読み出された暗号化されたソフトウェアを、フィルタ手段から出力されるソフト鍵を用いて復号化する。

【0024】請求項9に係る発明においては、記録媒体には、暗号化されたソフトウェアと、暗号化されたソフト鍵と、予め定められた制限回数と、今までにソフトウェアを実行した回数である実行回数とが格納されている。更新回数演算手段は、入力手段によってソフトウェアの追加したい実行回数が入力されると、記録媒体に格納された制限回数と実行回数との大小関係を考慮しつつ、当該追加実行回数に基づいて、制限回数の更新回数を演算する。また、制限回数書き換え手段は、更新回数演算手段により演算された更新回数によって、記録媒体

10

に格納された制限回数を書き換える。このように、予め定められた実行条件（制限回数）を、途中で自由に追加変更することができる。また、更新回数演算手段は、記録媒体に格納された制限回数と実行回数との大小関係を考慮しつつ、制限回数の更新回数を演算するようにしているので、たとえ実行回数が制限回数を越えていても、結果的に追加の実行回数が達成されるような正確な更新回数を演算できる。

【0025】

【実施例】

(1) 第1の実施例

図1は、本発明の第1の実施例に係るソフトウェア実行制御システムの構成を示すブロック図である。なお、以下の説明において、ソフトウェアとは、例えばアプリケーションプログラムを意味するものとする。図1において、ソフトウェア記録媒体としてのディスク1は、暗号化ソフトウェア記録部11と、情報記録部12とを含む。暗号化ソフトウェア記録部11には、暗号化ソフトウェアE (KA, soft A) が格納されている。情報記録部12には、ノイズ付きソフト鍵KA (+) Rと、制限回数Mと、実行回数CNTとが格納されている。なお、実行回数CNTは、各情報が読み出される毎に1ずつインクリメントされる。また、予め許可されたあるパスワードを知っている者しか、情報記録部12に格納されている情報を書き換えることはできない。上記ディスク1としては、磁気ディスク、光ディスク、MOD等が用いられる。また、ディスク1に代えて、不揮発性メモリにソフトウェアが格納されたメモリカートリッジを用いても良い。

【0026】プレーヤ2は、接続部21と、ソフト鍵復号処理部22と、暗号化ソフトウェア復号部23と、ソフトウェア実行部24とを備え、ディスク1内のノイズ付きソフト鍵KA (+) R、制限回数M、実行回数CNTを読み込んでソフト鍵KAを復号化し、ソフトウェアの実行を行う機能を有している。接続部21は、ディスク1をプレーヤ2に着脱自在に接続するもので、ディスク1から各情報を読み出す機能を有している。ソフト鍵復号処理部22は、情報記録部12に記録されているノイズ付きソフト鍵KA (+) Rを、同じく情報記録部12に記録されている制限回数M、実行回数CNTで復号化する機能を有している。暗号化ソフトウェア復号部23は、暗号化ソフトウェア記録部11に記録されているE (KA, soft A) が入力され、ソフト鍵復号処理部22で復号化されたソフト鍵で、当該暗号化ソフトウェアE (KA, soft A) を復号化する機能を有している。ソフトウェア実行部24は、暗号化ソフトウェア復号部23で復号化されたソフトウェアsoft Aを実行する機能を有している。

【0027】なお、図1のディスク1内における情報記録部12、プレーヤ2内におけるソフト鍵復号処理部2

11

2、暗号化ソフトウェア復号部23およびソフトウェア実行部24は、それぞれ変更、解析、複製できない領域に配置されている。また、プレーヤ2のオペレータは、パスワードを知らないで情報記録部12に記録されている情報を書き換えることはできない。

【0028】概説すると、上記第1の実施例のソフトウェア実行制御システムは、ソフトウェアs o f t A自体は、そのソフトウェアの全ディスク共通の鍵ソフト鍵KAで暗号化し、そのソフト鍵KAを実行回数CNTが制限回数Mを越えない場合に限り復号できるように復号化

することによって、実行回数を制限するようにしている。
【0029】なお、以下には、図1のディスク1をソフトウェア販売店から受け取る時に、予め実行する回数の限度である制限回数Mに応じた代金で購入した暗号化ソフトウェアE (KA, s o f t A) を、図1のプレーヤ2において制限回数Mと実行回数CNTの値によってソフト鍵KAを復号し、そのソフト鍵KAでソフトウェアs o f t Aを復号し実行する動作について説明する。また、以下の説明において、暗号化ソフトウェアE (KA, s o f t A) は、ソフトウェアs o f t Aをソフト鍵KAで暗号化したものを示し、ソフト鍵KAで復号化される。また、演算記号(+)は、ビット毎の排他的論理和を表しており、Rは本システム共通の値である。

【0030】次に、図2のフローチャートを参照して、*

$$KA' = f(KA (+) R, dis) \\ = \{KA (+) R\} (+) \{R * (dis + 1)\} \quad \dots (2)$$

ここで、KA' は、dis=0のとき、すなわちCNT<Mが成り立つときに限り、KAと等しくなる。

【0033】次に、ソフト鍵復号処理部22は、先に求めたKA' を、暗号化ソフトウェア復号部23に入力する(ステップS207)。暗号化ソフトウェア復号部23は、入力されたKA' で、暗号化ソフトウェアE (KA, s o f t A) を復号する(ステップS208)。なお、このとき、dis=0、すなわちCNT<Mが成り立たねば、KA' ≠KAとなり、ソフトウェアs o f t Aが復号できず、ソフトウェアは実行できない。

【0034】次に、暗号化ソフトウェア復号部23は、復号したソフトウェアs o f t Aを、ソフトウェア実行部24に入力する(ステップS209)。従って、ソフトウェア実行部204は、復号されたソフトウェアを実行する(ステップS210)。

【0035】以上説明したように、第1の実施例によれば、ソフトウェアを購入するときに定められた制限回数だけソフトウェアの実行を行うことができ、制限回数以上の実行を行うことは不可能である。従って、販売店としては、制限回数に見合う安い価格でソフトウェアパッケージを販売することができる。

【0036】なお、上記第1の実施例では、プレーヤ2がソフト鍵復号処理部22を備えているが、ディスク1

12

*上記第1の実施例のソフトウェア実行制御動作を説明する。まず、接続部21にディスク1が接続される(ステップS201)。次に、接続部21は、情報記録部12からノイズ付きソフト鍵KA (+) R、制限回数M、実行回数CNTを読み出し、これらをソフト鍵復号処理部22に入力する(ステップS202)。次に、接続部21は、情報記録部12に格納されている実行回数CNTを1だけ増やした値に更新する(ステップS203)。次に、接続部21は、暗号化ソフトウェア記録部11に格納されている暗号化ソフトウェアE (KA, s o f t A) を読み出し、暗号化ソフトウェア復号部23に入力する(ステップS204)。

【0031】次に、ソフト鍵復号処理部22は、制限回数Mと実行回数CNTから、次式(1)によって実行識別子disを計算する(ステップS205)。

$$dis = [CNT/M] \quad \dots (1)$$

ただし、上式(1)において、[] はガウス記号であり、[CNT/M] は、CNT/Mを越えない最大の整数を示している。なお、CNT<Mの場合、dis=0となる。

【0032】次に、ソフト鍵復号処理部22は、ノイズ付きソフト鍵KA (+) Rと、今求めたdisを、次式(2)で表される関数fに入力して、ノイズ付きソフト鍵のノイズを取り、KA' に変換する(ステップS206)。

を収納するカートリッジにチップを設け、このチップ内にソフト鍵復号処理部を設けるようにしてもよく、この場合も上記と同様の効果が得られる。この場合、ディスク1がプレーヤ2の接続部21に接続されたときに、暗号化ソフトウェアと、ソフト鍵復号処理部22で処理されたKA' とがディスク1からプレーヤ2に入力されることになる。

【0037】また、上記第1の実施例では、実行回数によってソフトウェアの実行を制限するようにしたが、実行日時によってソフトウェアの実行を制限するようにしても良い。この場合、ディスク1にはソフトウェアの使用終了日時となる実行停止日時を格納しておき、プレーヤ2にはタイマを設け、このタイマにより計時される現在の日時が上記実行停止日時の前の場合にのみ、ノイズ付きソフト鍵が正常に復号されるようにすればよい。なお、実行回数による制限と、実行日による制限とを組み合わせることで実行条件を制御することも容易に実現できる。

【0038】また、上記第1の実施例では、ディスク1にノイズ付きソフト鍵KA (+) Rを格納し、実行回数CNTが制限回数M以下の場合にのみノイズがとれるよう、ソフト鍵復号処理部22でノイズ付きソフト鍵を復号するようにしているが、逆に、ディスク1にノイズのないソフト鍵KAを格納し、実行回数が制限回数を越え

13

る場合のみソフト鍵KAにノイズが付加されるようにしても良い。この場合、プレーヤ2には、ソフト鍵復号処理部22に代えて、フィルタ回路が設けられ、このフィルタ回路は、実行回数CNTが制限回数M以下の場合にはディスク1から読み出したソフト鍵をそのまま暗号化ソフトウェア復号部23に出力し、実行回数が制限回数を越える場合はディスク1から読み出したソフト鍵にノイズを付加して暗号化ソフトウェア復号部23に出力する。

【0039】また、上記第1の実施例では、ディスク1に実行回数CNTと制限回数Mとを格納するようにしたが、これらに代えて、残りの実行可能回数を示す残高回数を格納し、ディスク1からの各データの読み出しに関連して残高回数を1ずつ減算するようにしても良い。

【0040】(2)第2の実施例

本発明の第2の実施例は、前述の第1の実施例のソフトウェア実行制御システムにおいて、ディスク購入時に設定された制限回数Mを、購入後に追加更新し得るシステムである。すなわち、前述の第1の実施例では、制限回数Mは、購入時に予め定められた回数としていた。そして、実行回数CNTが制限回数Mと等しいか、または大きいときに、KA'がKAと異なる値となり、暗号化ソフトウェアE(KA, software)が復号できないように構成されていた。これに対し、第2の実施例の追加更新システムは、ディスク1を購入後にソフトウェア販売店に持っていき、CNTとMの大小関係に関係なく、制限回数Mをユーザの望む回数だけ追加更新し得るシステムである。

$$M' = \max(M - CNT, 0) + CNT + add \quad \dots (3)$$

ただし、上式(3)において、 $\max(M - CNT, 0)$ は、 $M - CNT$ と0のうち小さくない方を表している。従って、上式(3)のM'は、 $M \geq CNT$ のとき、 $M' = M + add$
 $M < CNT$ のとき、 $M' = CNT + add$ となる。

【0045】次に、制限回数書換部33は、上記ステップS303で求めたM'を新しい制限回数Mとして、接続部31を介して、ディスク1内の情報記録部12に書き込む(ステップS304)。その後、ユーザは、ディスク1を持ち帰り、通常のとときと同様に使用する。

【0046】上記のように第2の実施例によれば、ソフトウェア販売店にディスク1を持って行き、ソフトウェアsoftwareの実行できる制限回数を新たに追加することが可能になる。また、式(3)によって追加更新数M'を決めているから、CNTがMより大きくなってから制限回数Mを更新しようとしても、また、まだMの方がCNTよりも大きい場合に制限回数Mを更新しようとしても、常にadd回だけ今までよりも多く実行できるような追加更新数M'を求めることができる。

【0047】なお、第2の実施例では、ディスク1をソ

14

*【0041】図3は、本発明の第2の実施例に係る追加更新システムの構成を示すブロック図である。図3において、追加更新装置3は、接続部31と、更新回数演算部32と、制限回数書換部33とを備え、ディスク1内の情報記録部12に記録されている制限回数Mを更新する機能を有している。

【0042】図4は、上記第2の実施例の追加更新システムにおける処理手順を示すフローチャートである。以下、この図4を参照して、第2の実施例の詳細を説明する。

【0043】ユーザは、ディスク1を持ってソフトウェア販売店に行く(ステップS301)。第1の実施例で述べたように、ディスク1内の情報記録部12に記録されている情報は、予め許可されているものしか変更できない。ソフトウェア販売店のオペレータは、情報記録部12に記録されている記録を書き換えるためのパスワードを知っており、当該パスワードを追加更新装置3に入力することにより、情報記録部12に記録されている情報を書き換えることができる。

【0044】ユーザは、新たに実行したい追加回数addをソフトウェア販売店のオペレータに知らせる(ステップS302)。ソフトウェア販売店のオペレータは、当該追加回数addを追加更新装置3に入力する。応じて、追加更新装置3内の更新回数演算部32は、ディスク1内の情報記録部12に記録されている実行回数CNTと制限回数Mに対して、次式(3)で表されるM'を計算する(ステップS303)。

ソフトウェア販売店に持って行き、制限回数Mの追加更新を行っているが、オンラインでソフトウェア販売店の追加更新装置3とつながっているシステムを考えるならば、オンラインで制限回数Mの追加更新を行うことも出来る。

【0048】

【発明の効果】請求項1～3の発明によれば、記録媒体に格納された実行回数が制限回数以下の場合にのみ、記録媒体から読み出された暗号化されたソフト鍵を正常に復号するようにしているので、ソフトウェアの実行回数を予め定められた回数に制限することができる。従って、販売店としては、販売時に定めた回数に見合う安い価格でソフトウェアパッケージを販売することが可能となり、その分ユーザの価格負担を軽減できる。

【0049】請求項4の発明によれば、記録媒体に格納された残高回数が1以上の場合にのみ、記録媒体から読み出された暗号化されたソフト鍵を正常に復号するようにしているので、ソフトウェアの実行回数を予め定められた回数に制限することができる。従って、販売店としては、販売時に定めた回数に見合う安い価格でソフトウェアパッケージを販売することが可能となり、その分ユ

15

ーザの価格負担を軽減できる。

【0050】請求項5の発明によれば、記録媒体に格納された実行回数が制限回数以下の場合は、記録媒体から読み出されたソフト鍵をそのまま出力し、当該実行回数が制限回数を越える場合は、当該ソフト鍵に所定のノイズを付加して出力するようにしているので、ソフトウェアの実行回数を予め定められた回数に制限することができる。従って、販売店としては、販売時に定めた回数に見合う安い価格でソフトウェアパッケージを販売することが可能となり、その分ユーザの価格負担を軽減できる。

【0051】請求項6の発明によれば、記録媒体に格納された残高回数が1以上の場合は、記録媒体から読み出されたソフト鍵をそのまま出力し、当該残高回数が0以下の場合は、当該ソフト鍵に所定のノイズを付加して出力するようにしているので、ソフトウェアの実行回数を予め定められた回数に制限することができる。従って、販売店としては、販売時に定めた回数に見合う安い価格でソフトウェアパッケージを販売することが可能となり、その分ユーザの価格負担を軽減できる。

【0052】請求項7の発明によれば、タイマ手段により計時された現在の日時が記録媒体から読み出された実行停止日時よりも時間的に前の場合にのみ、記録媒体から読み出された暗号化されたソフト鍵を正常に復号するようにしているので、ソフトウェアの実行期間を予め定められた日数に制限することができる。従って、販売店としては、販売時に定めた制限日数に見合う安い価格でソフトウェアパッケージを販売することが可能となり、その分ユーザの価格負担を軽減できる。

【0053】請求項8の発明によれば、タイマ手段により計時された現在の日時が記録媒体から読み出された実行停止日時よりも時間的に前の場合は、記録媒体から読み出されたソフト鍵をそのまま出力し、現在の日時が実行停止日時よりも時間的に後の場合は、当該ソフト鍵に所定のノイズを付加して出力するようにしているので、ソフトウェアの実行期間を予め定められた日数に制限す *

16

*ることができる。従って、販売店としては、販売時に定めた制限日数に見合う安い価格でソフトウェアパッケージを販売することが可能となり、その分ユーザの価格負担を軽減できる。

【0054】請求項9の発明によれば、記録媒体に記録されたソフトウェアの実行条件である制限回数を、ソフトウェアの実行後も自由に追加更新することができる。また、更新回数演算手段は、記録媒体に格納された制限回数と実行回数との大小関係を考慮しつつ、制限回数の更新回数を演算するようにしているので、たとえ実行回数が制限回数を越えていても、結果的に追加の実行回数が確実に達成されるような正確な更新回数を演算できる。

【図面の簡単な説明】

【図1】本発明の第1の実施例に係るソフトウェア実行制御システムの構成を示すブロック図である。

【図2】本発明の第1の実施例のソフトウェア実行制御システムにおける処理手順を示すフローチャートである。

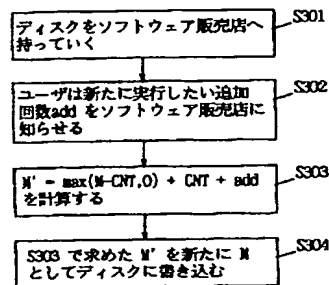
【図3】本発明の第2の実施例に係る追加更新システムの構成を示すブロック図である。

【図4】本発明の第2の実施例の追加更新システムにおける処理手順を示すフローチャートである。

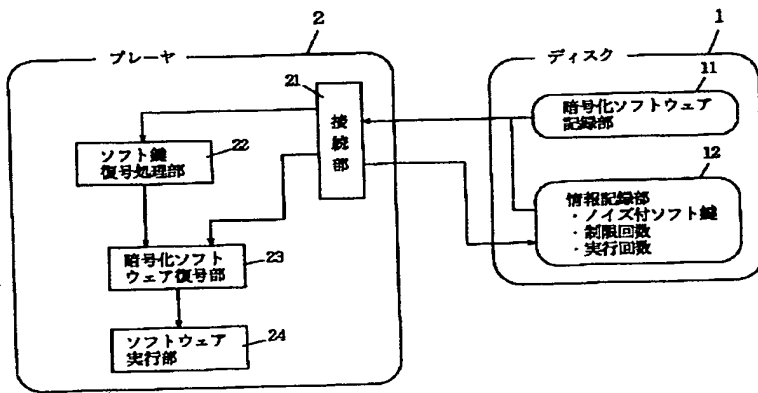
【符号の説明】

- 1…ディスク
- 11…暗号化ソフトウェア記録部
- 12…情報記録部
- 2…プレーヤ
- 21…接続部
- 22…ソフト鍵復号処理部
- 23…暗号化ソフトウェア復号部
- 24…ソフトウェア実行部
- 3…追加更新装置
- 31…接続部
- 32…更新回数演算部
- 33…制限回数書換部

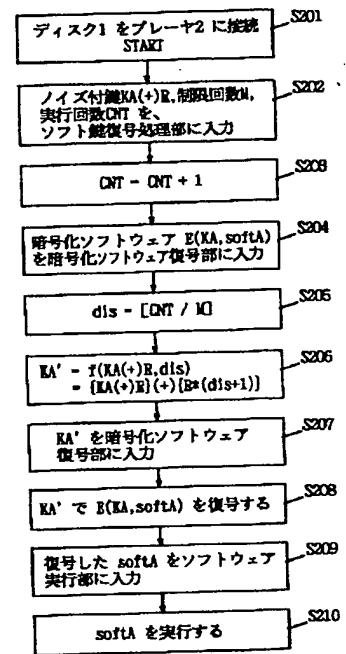
【図4】



【図 1】



【図 2】



【図 3】

